Available online at www.sciencedirect.com
ScienceDirect
Procedia Computer Science 79 (2016) 553 – 560
Procedia Computer Science

7th International Conference on Communication, Computing and Virtualization 2016

Analysis of Knowledge Based Authentication System Using Persuasive Cued Click Points

Atish Nayak[1] , Rajesh Bansode[2]

PG Student, Department of IT,TCET, kandivali,Mumbai-400101 India[1]
Assistant Professor, Department of IT,TCET kandivali, Mumbai-400101 India[2]

Abstract

In general users tend to choose memorable passwords that are easy for attackers to guess, but strong system assigned passwords are hard for users to remember. In this paper focuses on the integrated evaluation of the Persuasive Cued Click Points graphical password system which including usability and security evaluation on three different level. An important goal of authentication systems is support users in selecting better passwords. Increasing security by expanding the value of effective password space. In the click-based graphical passwords, poorly chosen passwords lead to the emergence of hotspots (image portions where users are more likely to select click-points, allowing attackers to mount more successful dictionary attacks). This paper used persuasion to influence user choice is used in click-based graphical passwords for encouraging users to select more random, and hence more difficult to guess, click-points.

Peer-review under responsibility of the Organizing Committee of ICCCV 2016

Keywords: Authentication, usable security, empirical studies, persuasive technology, graphical passwords.

1. Introduction

There are many things which are well known about the passwords such that user cannot remember strong password and the passwords which user can remember are easy to guess [1]-[3].

The password authentication system should encourage strong and less predictable passwords with maintaining memorability and security. This password authentication system allows user choice while influencing users to select stronger passwords. The task of selecting weak passwords (which is easy for attackers to guess) is more tedious, users need to avoid making such choices. In effect, this authentication schemes makes choosing a more secure password the path-of-high-resistance. Rather than increasing the burden on users, it is easier to follow the system's suggestions for the secure password (a feature absent in most schemes).

The approach is to generate the persuasive click-based graphical password system, conducted an in lab study (lab usability study with 20 participants). The results reported indicate that our Persuasive Cued Click Points scheme is effective for the reducing the numbers of hotspots [2]-[3] (The areas of the image where users are more likely to select click points) while still maintaining usability. In this paper, the efficiency of tolerance value and security rate is analyzed. While it is discussed that graphical passwords are the best approach to authentication as they offer an excellent environment for exploring strategies in helping users select better passwords as it is easy to compare user choices. Indeed, it is mentioned how the approach is adapted to text-based passwords.

2. Background

Text passwords are most using user authentication method, but it has security and usability problems. Replacements like biometric systems and tokens have their own drawbacks [1]-[3]. Graphical passwords offer another alternative which are the focus of this paper. The graphical passwords were originally defined by Blonder in 1996 [3]. In general, graphical passwords techniques are classified into two different categories which are recognition-based and recall based graphical techniques. In the recognition

Corresponding author. Tel.+91- 9820271046;
E-mail address: rajesh.bansode@thakureducation.org

Peer-review under responsibility of the Organizing Committee of ICCCV 2016
doi:10.1016/j.procs.2016.03.070

based techniques, user is presented with a set of images and the user passes the authentication by the identifying and recognizing the images user selected during the registration stage. In the recall based graphical password the user is asked to regenerate something which is generated or selected by user earlier during the registration process. This project is based on the recall based Technique.

The problem of knowledge-based authentication system is typically text-based passwords that are well known. Users often create the memorable passwords that are easy for attackers to predict but strong system assigned passwords are difficult to remember for the users.

A password authentication system encourages strong passwords while maintaining memorability. IT is proposed that authentication schemes allow user choice to use strong passwords. In the system, task of selecting weak passwords is more tedious which is turn into discourages users from making such choices. This approach makes selection of more secure password as the path of high resistance. Instead of increasing the burden on users, It is easier for user to follow the system's suggestions for the secure password—a feature lacking in most schemes.

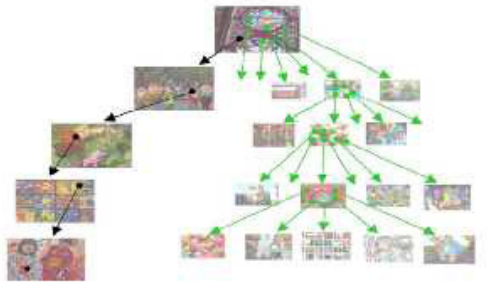

Fig. 1 User navigation trough images to form a PCCP password

This approach is to create the persuasive click-based graphical password system, Persuasive Cued Click-Points (PCCP) that conducts user studies evaluating usability and security. The current paper presents a consistent assimilation of earlier work and two web studies that reinterprets and updates statistical analysis incorporating larger data sets which provides new evaluation of password distributions. It extends security analysis including relevant recent attack and presents important implementation details.

The systematic examination provides a comprehensive and integrated evaluation of PCCP covering both usability and security issue, to advance understanding before practical deployment of new security mechanisms. Through eight user studies, the comparison is done PCCP to text passwords and two related graphical password systems. Results state that PCCP is effective at reducing hotspots and avoiding patterns formed by click-points within a password, while maintaining usability.

I. Click-Based Graphical Passwords

The graphical password systems are a type of knowledge-based authentication that attempts to use the human memory for visual information. The complete review of graphical passwords is available elsewhere. The interest herein is cued-recall click-based graphical passwords (which is also known as the loci metric). In such systems, users identify and target previously selected locations within one or more than one images. Here the images act as memory cues to aid recall. Example systems include Cued Click-Points (CCP) [4] and the Pass Points [5].

In the Pass Points, a password consists of a sequence of five click-points on a given image (refer Fig. 2). The users may select pixels in the image as click-points for their password. To log in, they repeat the sequence of clicks in the correct order, in a system-defined tolerance square of the original click-points. The usability and security of this scheme was evaluated by the original authors and subsequently by others. It was found that although relatively usable, security concerns remain. Primary security problem is hotspots: different users tend to select similar click-points as part of the passwords. The attackers who gain knowledge of these hotspots through harvesting sample passwords or via automated image processing techniques can build attack dictionaries and more successfully guess Pass Points passwords. The dictionary attack consists of using a list of potential passwords (ideally in decreasing order of likelihood) and trying that the system in turn to see if system leads to a correct login for a given account. Attacks can target a single account, or they can try guessing passwords on a large number of accounts in hopes of breaking into any of them.

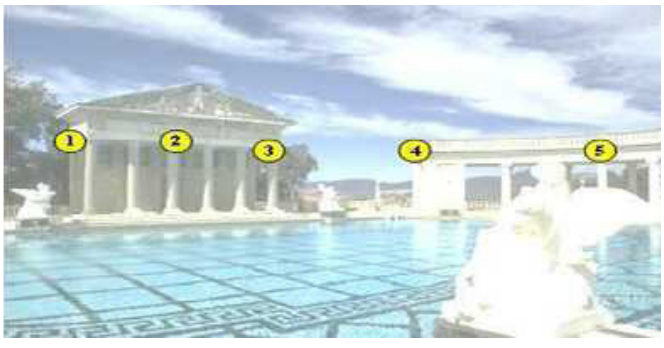

Fig. 2 pass point (contain 5 point on single image)

In PCCP, Cued Click Points was designed to reduce the patterns and to reduce the usefulness of hotspots for the attackers. In the place of five click-points on one image, CCP uses one click-point on five different images which is displayed in sequence. Next image shown is based on the location of previously entered click-point (refer Fig. 3), creating the path through an image set. Users can select their images only to the extent that click-point shows the next image. For creating a new password with different click-points results in a different image sequence [6].

The main advantages are that password entry becomes the true cued-recall scenario, where every image triggers the memory of each corresponding click-point. For remembering the order of the click-points is no longer a requirement on users, the system presents the images one at a time. The CCP also provides implicit feedback claimed for useful only to legitimate users. When log on in system, seeing an image they do not identify alerts users that the previous click-point was incorrect and users may restart the password entry. The explicit indication of authentication failure is provided after the final click-point, for the protect against incremental guessing attacks.

User testing and analysis showed no evidence of the patterns of CCP, so pattern-based attacks seem ineffective. The attackers Have to perform proportionally more work to exploit hotspots, results displayed that hotspots remained a problem [7] .

Fig. 3 click points as a password

II. Persuasive Technology

Persuasive technology was first articulated by the Fogg [8] as using technology to motivate and influence people for the behave in a desired manner. An authentication system which applies persuasive technology should guide with encourage the users for selecting the stronger passwords, but not impose system-generated passwords. For being effective, the users must not ignore the persuasive elements and resulting passwords must be memorable [9].

PCCP accomplishes it by making the task of selecting a weak password more tedious and time consuming. The path of most resistance for users is to select a stronger password (not comprised entirely of known hotspots or following the predictable patterns). Formation of hotspots across users is minimized since click-points are more randomly distributed.). In result, the system also has the advantage of minimizing the formation of hotspots across users since click points are more randomly distributed [10]-[12].

3. PERSUASIVE CUED CLICK POINTS

The previous models have displayed that hotspots are the problem in click-based graphical passwords, which is leading to decrease the effective password space which facilitates more successful dictionary attacks. In this paper investigated that whether password choice could be influenced by persuading users to select more random click-points while still maintaining usability. The main goal was to encourage compliance by making the less secure task (i.e., choosing the poor passwords) more time consuming and complicated. For behaving securely became the path-of-high-resistance.

By using the CCP as a base system here added a persuasive feature to making users to select high secure passwords, and to make it difficult for selecting the passwords where all five click-points are hotspots. Specifically, when users created a password, Images which slightly shaded except for a randomly positioned viewport (refer Fig. 4). The viewport is positioned randomly except than specifically to avoid known hotspots, such information could be used by attackers to improve the guessing which could also lead to the formation of new hotspots. The viewport's size was intended to offer a variety of the points but still cover only an acceptably small fraction of all possible points. Users were required to select the click point within this highlighted viewport and could not click outside of this viewport. If they were unwilling or unable to select the click point in the region, they could press the "shuffle" button to randomly reposition the viewport. The users were allowed to shuffle as often as they wanted, this significantly slowed the password creation process. Viewport and shuffle buttons appeared during password creation. During password confirmation, login and images were displayed normally, without shading of the viewport and users were allowed to click anywhere.

Our hypotheses were

a) Users have multiple choices for security according to their need by using multiple viewpoints.
b) User will feel less fear that the selected point is not known hotspot.
c) The click-point distribution with users will be randomly dispersed and will not generate the new hotspots.
d) The login security success rates will be higher than to those of the original CCP system.
e) The login security success rates will increase, when viewpoint get decreased.
f) Participants will feel that their passwords are more secure with PCCP than participants of the original CCP system.

Fig. 4 PCCP Create Password interface

The theoretical password space for the password system is equal to the total number of unique passwords that could be generated according to the system specifications. The larger theoretical password space lowers the likelihood that any particular guess is correct for the given password. In PCCP, the theoretical password space is $((w \times h)/t^2)^c$ where the size of the image in pixels (w * h) which is divided by the size of a tolerance square (t^2), for the getting the total number of tolerance squares per image, which is raised to the power of the number of click-points in a password (c, usually set to 5 in our experiments).

4. SYSTEM DESIGN

The system designed consist of three modules such as user registration module, picture selection module and system login module (refer Fig. 5).

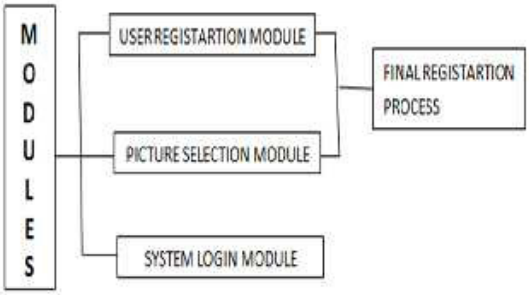

Fig. 5 System modules

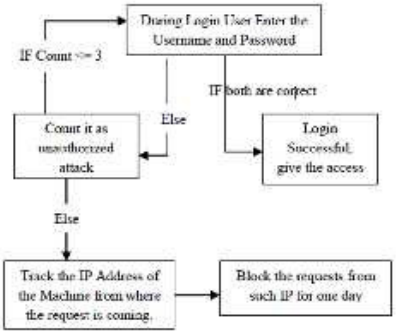

Fig. 6 system login module

a) In the user registration module user can enter the user name in user name field which is also suitable tolerance value (tolerance value which is use to compare registration profile vector with the login profile vector). When the user entered the all user details in the registration phase, these user registration data stored in the data base which used during login phase for the verification.

b) In the picture selection phase user select any image as passwords and consist of a sequence of five click-points on a given image. The users may select any pixels in the image as click-points for their password. During password creation in that most of the image is dimmed except for a small view port area that is randomly positioned on the image. Users have to select the click-point within the view port. For that they are unable or unwilling to select the point in the current view

port, users may went for the Shuffle button to randomly reposition of the view port. The view port indicates users to select more random passwords which are less likely to include hotspots. The user who is determined to certain click-point may still shuffle until the view port reach to the specific location, but this is a time consuming and more difficult process.

c) During system login, the images are displayed normally, without viewport, and repeat the sequence of clicks in correct order, with a system-defined tolerance square of the original click-points.

I. User registration flow chart

Below flowchart (refer Fig. 7) shows the user registration procedure, this procedure contain the both registration phases and picture selection phase. Process flow starts from registering user id and the tolerance value. When user completes all user details then proceeds to next stage, which is selecting click points on the generated images, which is range in between 1 to 5. After done all above procedure, user profile vector will be created.

II. Login flow chart

In this login procedure (refer fig. 8), first user enters the unique user ID as same as entered during registration. The images are displayed normally, By shading or the viewport, and repeat the sequence of clicks in the correct order, with the system-defined tolerance square of the original click-points. After done with all the procedure seen above, user profile vector will be opened.

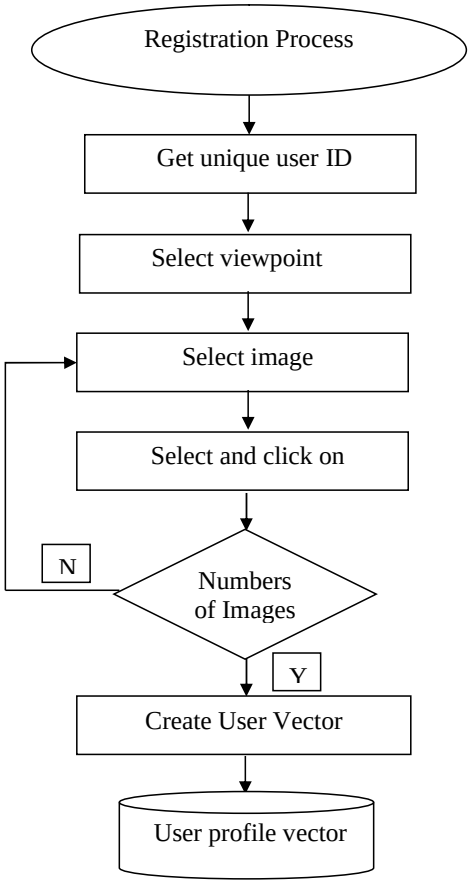

Fig. 7 User registration flowchart

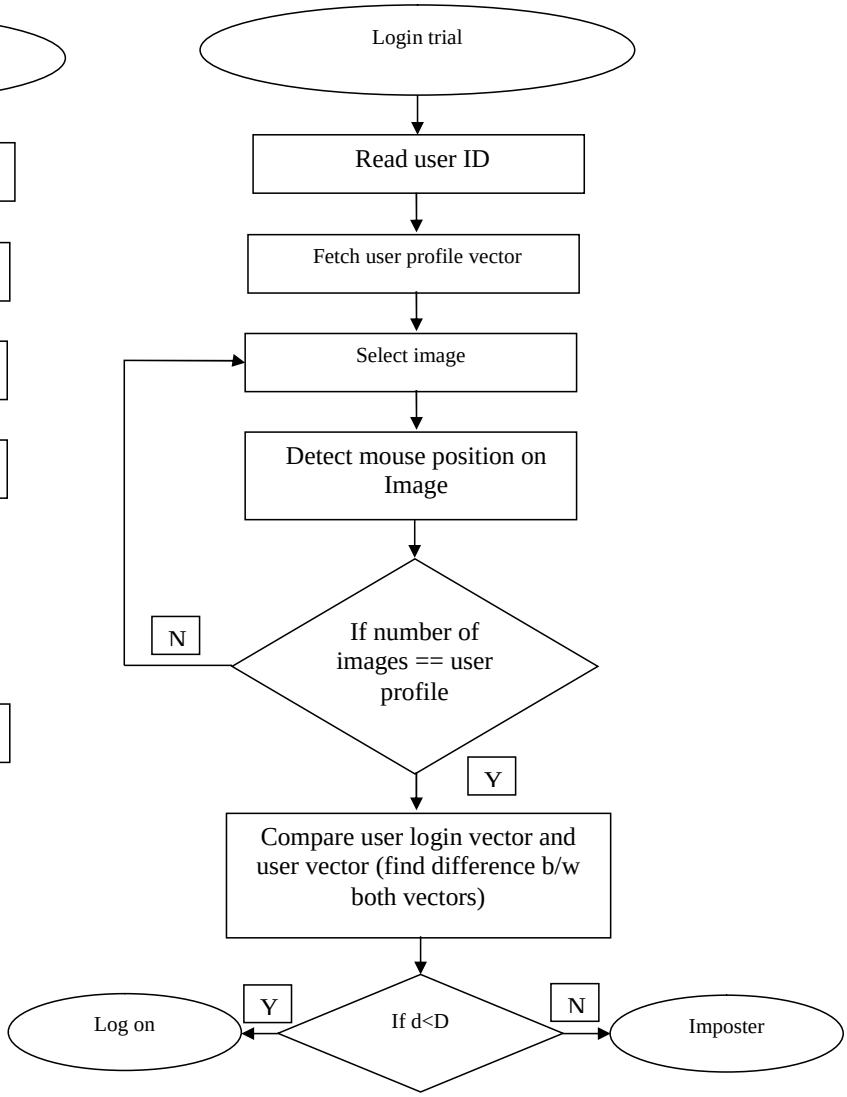

Fig. 8 Login phase flowchart

5. RESULTS

The empirical study was designed to explore ways of increasing the efficiency of tolerance value and also conducted lab study for the comparison of login success rate vs. security success rate of existing CCP's and proposed PCCP's.

I. Efficiency of the tolerance value

Initially eight participants are considered for the experiment. Each participant has a password which includes clicking on 5 click points in 5 different images. Each image consists of different characters (image details), among which the participant needs to click on any one point of user's choice to make the click point in the series. Similarly, the participant select a click point each of the images. Then, the participant log in with the password, meantime the other participants are made to stand in a group behind the participant who is entering password and are made to peek in over the shoulder of the participant and observe his password (the click points on the images)[14]. Once the first participant has logged out, the other participants are asked to enter same password which they have observed for the first participant.

Tolerance value: It is the value which indicates the degree of closeness to the actual click point.

Tolerance region: The area around an original click point accepted as correct since it is unrealistic to expect user to accurately target an exact pixel.

Success rate: It is the rate which gives the number of successful trails for a certain number of trials. the success rates are calculated as the number of trails completed without errors or restarts.

Shoulder surfing: It is the process by which the person standing behind the person entering the password observes the password. It is a type of capture attack. This attack occurs when attackers directly obtain the passwords (or parts thereof) by intercepting the user entered data or by tricking users into revealing their passwords.

The below table I shows the result of the tolerance value efficiency of the PCCP method. The results show the graph of the tolerance value against security success rate (refer fig. 9) and the graph of tolerance value against success rate(refer fig. 10).

Table I Efficiency of tolerance value in PCCP method

Sl. No	Tolerance Value	Success Rate	Percentage of success rate	Security (in percentage)
1	5	7/8	87.5	12.5
2	4	5/8	62.5	37.5
3	3	3/8	37.5	62.5
4	2	2/8	25	75
5	1	0/8	0	100

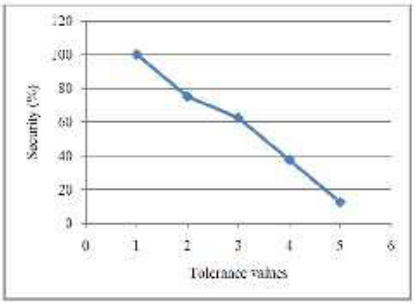

Fig. 9 Security increases with decrease in the tolerance value.

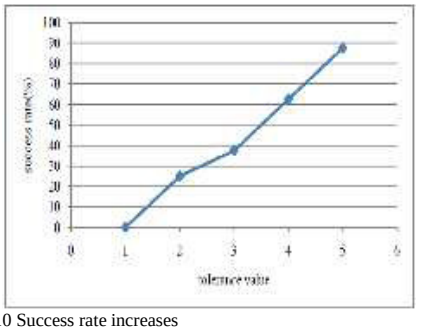

Fig. 10 Success rate increases with increase in the tolerance value

II. Comparison between login Success rate and security success rates of existing CCP and proposed PCCP

Success rates are reported with the first attempt and within three attempts. Success on the first attempt occurs when the password is entered correctly on the first attempt, without any mistakes. Success rates within three attempts indicate that fewer than three mistakes. Mistakes occur when the participant presses the Login button but the password is incorrect.

Table II PCCP success rates (all level) and security success rates compared to CCP

	CCP		PCCP (100*100 VP)		PCCP (75*75 VP)		PCCP (50*50 VP)	
	Success rate (%)	**Security Success rate (%)**	**Success rate (%)**	**Security success rate (%)**	**Success rate (%)**	**Security Success rate (%)**	**success rate(%)**	**Security Success rate(%)**
User1	4/5 (80)	20	3/5 (60)	40	4/5(80)	20	2/5(40)	60
Usre2	3/5 (60)	40	2/5 (40)	60	2/5(40)	60	3/5(60)	40
User3	5/5 (100)	0	4/5 (80)	20	2/5(40)	60	2/5(40)	60
		20 (mean rate)		40 (mean rate)		70 (mean rate)		80 (mean rate)

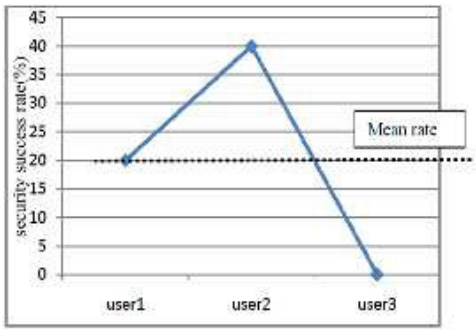

Fig.11 CCP mean rate

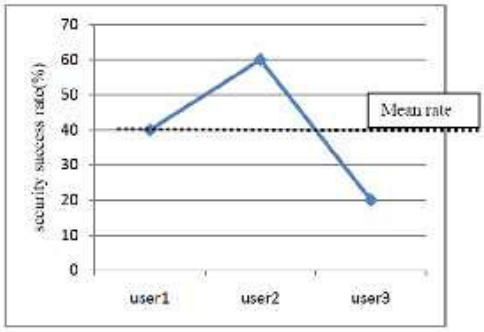

Fig. 12 PCCP mean rate

To conducted question answer round with 20 people, The scores for those questions were reversed prior to calculating the means and medians, thus higher scores always indicate more positive results for PCCP in Table III.

Table III Questionnaire responses. Scores are out of 10

Query	**View point 100*100**	**View point 75*75**	**View point 50*50**
I could easily create a graphical Password	8	8	7.5
Logging on using a graphical password was easy	6.4	7	8.3
Graphical passwords are easy to Remember	6	5.7	5
I prefer text passwords to graphical Passwords	4.9	5	5.2
Text passwords are more secure than graphical passwords	6	6.2	6.5
I think that other people would choose different points than me for a graphical password	7.2	7	8
With practice, I could quickly enter my graphical password	8.3	8	7.2

8. CONCLUSION

The most important usability and security goal in the authentication systems is to help the user for the selecting better passwords and increasing the effective password space. Users can be persuaded for the selecting stronger passwords through the better user interface design. For the example, the design of the Persuasive Cued Click-Points (PCCP) and conducted the usability

study for the evaluate its effectiveness. Here we obtained favourable results both for and security for three different viewpoints.

The PCCP encourages and guides users into selecting the more random click-based graphical passwords. The key feature in PCCP is to creating a secure password is the “path-of-high-resistance”, making it to be more effective than schemes where behaving securely adds one more extra burden on users. Approach has proven effective at reducing the formation of hotspots and avoid the shoulder surfing problem and also provide high security success rate, while still maintaining usability.

REFRENCES

[1] S.B.Sahu, A. Singh “Survey on Various Techniques of User Authentication and Graphical Password,” published in International Journal of Computer Trends and Technology (IJCTT), vol.16, pp 98-102, no.3, Oct. 2014.
[2] S. Chiasson, A. Forget, O. Biddle, P.C. van Oorschot “Persuasive Cued Click-Points: Design, Implementation, and Evaluation of a Knowledge-Based Authentication Mechanism,” published in IEEE transactions on dependable and secure computing, vol. 9, no. 2, pp.222-235, Apr. 2012.
[3] S. Chiasson, A. Forget, O. Biddle, P.C. van Oorschot “Influencing Users Towards Better Passwords: Persuasive Cued Click-Points,” Published in Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction, vol.1, sep. 2008, pp.121-130.
[4] S.B.Sahu, A. Singh “Secure User Authentication & Graphical Password using Cued Click-Points,” published in International Journal of Computer Trends and Technology (IJCTT), vol.18, no.4, pp.156-160, Dec. 2014.
[5] Usha T, Tara H R, G I Shidaganti “Knowledge Based Authentication Mechanism Using Persuasive Cued Click Points,” published in International Journal of Engineering Research & Technology (IJERT), vol. 2, no 6, pp.258-266, Jun. 2013.
[6] A. Cummings 2012, Insider Threat Study: Illicit Cyber Activity Involving Fraud in the U.S. Financial Services Sector [online], Available: http://www.sei.cmu.edu/reports/12sr004.pdf
[7] G. Niranjana, K. Dawn “Graphical Authentication using Region based Graphical password,” published in International Journal of Computer Science and Informatics ISSN, vol.2, no.3, pp.114-119, feb.2012.
[8] G. Niranjana, K. Dawn “A Novel Gesture Based Graphical Authentication Using Bounding Box and Corner Detection Algorithm,” published in International Journal of Computer Science and Informatics ISSN, vol.12, no.3, pp.114-119, Nov. 2012.
[9] U. D. Yadav, P. S. Mohod “Adding Persuasive features in Graphical Password to increase the capacity of KBAM,” Published in IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology, vol.2, Mar.2013, pp.513-517.
[10] S. Chiasson, A. Forget, O. Biddle, P.C. van Oorschot “Improving Text Passwords Through Persuasion,” Published in Symposium on Usable Privacy and Security (SOUPS), vol. 4, pp.1-12, Jul. 2008.
[11] Wei-Chi Ku, Dum-Min Liao, Chia-Ju Chang, Pei-Jia Qiu “An Enhanced Capture Attacks Resistant Text-Based Graphical Password Scheme,” Published in Symposium on Privacy and Security in Commutations, vol.4, pp.204-208, Oct.2014.
[12] S. Chiasson, C. Deschamps, E. Stobert, M. Hlywa, B. Freitas Machado, A. Forget, N. Wright, G. Chan, and R. Biddle, “ The MVP Web-Based Authentication Framework,” Published in Proc. Financial Cryptography and Data Security (FC), LNCS, vol.7397, pp 16-24, Mar.2012.
[13] V. Kumar, M. K. Gupta, A. Chaturvedi, A. Bhardwaj, M. P. Singh “Click to Zoom-inside Graphical Authentication,” Published in International Conference on Digital Image Processing, vol.4, no.2, Mar.2009, pp.238-242.
[14] Paul C. van Oorschot, A Salehi-Abari, J. Thorpe “Purely Automated Attacks on PassPoints-Style Graphical Passwords,” Published in IEEE transactions on information forensics and security, vol. 5, no. 3, pp. 393-405, Sep. 2012.
[15] S. Chiasson, A. Forget, O. Biddle, P.C. van Oorschot “User interface design affects security: patterns in click-based graphical passwords,” Published in International Journal of Information Security, vol.8, no.6, pp. 387-398, May 2009.
[16] V. D. Bhong M.R.Shahade “Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice,” Published in International Journal for Engineering Applications and Technology, vol.5, pp. 239-245, Feb. 2013.
[17] B. Fogg, “Persuasive Technologies: Using Computers to Change What We Think and Do”, Morgan Kaufmann Publishers, vol.2002, no.5, Dec. 2003.
[18] Persuasive technology “Computer and Network Security,” [Online], Available: https://en.wikipedia.org/wiki/Persuasive_technology.pdf